CUMULOCITY

WHITE PAPER

NAVIGATING THE EU CYBER RESILIENCE ACT

What smart equipment manufacturers need to know

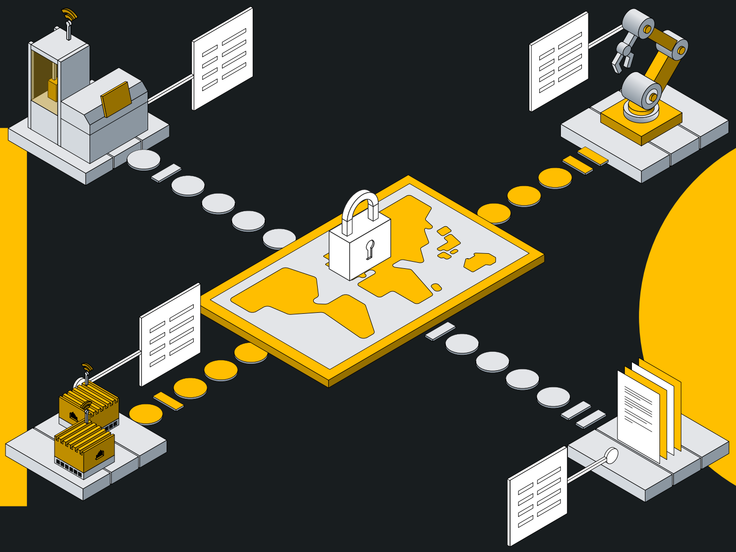


Table of contents

3 Introduction

3 Understanding the Cyber Resilience Act

4 Timelines and Penalties

4 - 5 Key Considerations for CRA Compliance

6 Best Practices for Building Cyber-Resilient Smart Equipment

6 What Manufacturers Need to Do Next

7 How Cumulocity Helps Manufacturers Meet CRA Requirements

7 Conclusion

7 Take the next step

8 Manufacturer CRA Checklist

8 Appendix / Resources

Executive Summary

The EU Cyber Resilience Act (CRA) introduces mandatory cybersecurity requirements for all products with digital elements. It compels manufacturers to embed security by design, monitor for vulnerabilities throughout the product lifecycle, and ensure their products can be updated securely when needed.

For smart equipment makers, this regulation is both a challenge and an opportunity. Compliance requires secure development practices, software inventory tracking, and readiness to respond to vulnerabilities. Non-compliance risks fines of up to €15 million or 2.5% of global turnover, as well as potential removal from the EU market.

However, early adopters can turn CRA readiness into a competitive advantage. By building more secure and reliable connected products, manufacturers can win customer trust and strengthen their position in an increasingly security-conscious market.

Key milestones are approaching fast. The CRA entered into force on 10 December 2024. Mandatory reporting obligations for vulnerabilities and incidents will apply from 11 September 2026, and the full set of product requirements will apply from 11 December 2027. For manufacturers whose product development and testing cycles span years, preparation must begin now.

Introduction

Smart equipment has become deeply connected. Industrial machinery, medical devices, and building automation systems now rely on complex software stacks, cloud services, and third-party integrations. While connectivity unlocks new capabilities, it also expands the attack surface for cyber threats.

The European Union created the Cyber Resilience Act to raise the baseline for cybersecurity. Unlike fragmented national rules or voluntary guidelines, the CRA enforces a single, harmonized set of obligations across the EU market. It shifts the responsibility for security firmly onto manufacturers, ensuring that connected devices are secure by design and remain secure throughout their lifecycle.

For manufacturers of connected equipment, the implications are clear. Products that fail to meet CRA requirements may be removed from the market. Vulnerabilities must be monitored and mitigated. Compliance will require new processes for development, supply chain management, and post-market support.

This white paper is written for smart equipment manufacturers, IoT leaders, product managers, and compliance teams who need to understand the CRA's requirements and what they mean in practice.

Understanding the Cyber Resilience Act

The CRA applies to any "product with digital elements," covering everything from consumer IoT devices to industrial equipment and embedded software. Its core objective is to ensure that security is not optional but an integral part of how connected products are built and maintained.

Scope and Obligations

Under the CRA, manufacturers must:

- **Design and ship secure products by default.** Devices must include strong authentication, encrypted communications, secure boot, and safe default configurations.
- **Establish vulnerability management processes.** Manufacturers must monitor vulnerabilities across all product components and issue timely security updates to mitigate risks, with updates installed automatically where possible. Additionally, manufacturers must implement a **coordinated vulnerability disclosure (CVD) policy**, enabling the public to report vulnerabilities even if they have not been exploited. This differs from mandatory incident reporting to authorities and is essential for fostering transparency and proactive risk mitigation.
- **Report actively exploited vulnerabilities.** If a vulnerability is exploited, it must be reported to the EU Agency for Cybersecurity (ENISA) within 24 hours, with a detailed risk assessment submitted within 72 hours.
- **Demonstrate compliance through conformity assessments and CE marking.** For standard products, manufacturers can typically self-assess. However, 'Important' or 'Critical' products require assessments involving a third-party notified body.

Manufacturers must define a support period during which they will manage vulnerabilities. This must be at least five years unless the expected product lifetime is shorter.

Timelines and Penalties

The regulation entered into force in December 2024. Some obligations — such as vulnerability handling — will apply by 2026. Full compliance becomes mandatory on 11 December 2027.

Failing to comply carries significant consequences. Products may be withdrawn from the EU market, and manufacturers may face fines of up to €15 million or 2.5% of global annual turnover.

Key Considerations for CRA Compliance

To meet the CRA's requirements, manufacturers must adopt a holistic, lifecycle-driven approach. Six areas deserve particular focus:

1. Documentation and Evidence of Compliance

CRA compliance starts with documentation. Manufacturers must:

- Maintain a full product inventory
- Provide publicly accessible documentation, including instructions for secure decommissioning (per Article 31, Annex II)
- Keep detailed records of software changes, updates, vulnerability assessments, and incident response actions

This documentation is essential to pass conformity assessments and audits — and is often the starting point for any CRA readiness journey.

2. Secure Development Processes and Risk Assessment

Manufacturers must embed secure development practices, supported by product-specific risk assessments. These guide the choice and implementation of security controls — such as threat modelling, secure coding, and software signing.

3. Product Security

Based on the risk assessment, technical controls must be implemented, such as:

- Secure boot
- Authenticated and encrypted updates
- Enforced safe defaults
- Tamper resistance mechanisms
- Secure factory reset functionality

These should be integrated into the product architecture from the earliest design stages.

4. Software Update and Vulnerability Management

Manufacturers must monitor for vulnerabilities across all software components — first-party, third-party, and open source — and provide secure updates that:

- Are cryptographically verified
- Separate security patches from functional updates
- Support version rollback where feasible

Proactive vulnerability management requires clear ownership, automated monitoring tools, and rapid response capabilities.

5. Incident Response anvorting

Manufacturers must report exploited vulnerabilities and serious incidents to ENISA and their national CSIRT, with timelines as follows:

- Initial alert within 24 hours
- Full technical report within 72 hours
- Final status report within 14 days of mitigation

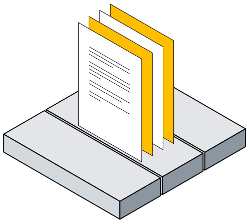
This demands a well-defined incident response plan that spans technical, legal, and communications teams.

6. Supply Chain Responsibilities and Third-Party Components

CRA applies to open-source components, commercial libraries, and supply chain integrations. Manufacturers must:

- Maintain full component-level visibility (e.g. SBOMs)
- Continuously assess exposure to disclosed vulnerabilities
- Accept legal responsibility for third-party and open-source code used in their products

Importers and distributors also carry CRA obligations. If they modify or rebrand a product, they may assume full manufacturer responsibilities. Manufacturers must also manage “substantial modifications” — changes that impact compliance or intended use.



READ OUR CRA TECHNICAL WHITEPAPER

Dive deeper into how Cumulocity helps you meet CRA requirements.

Including architecture diagrams, feature breakdowns, and best practices for smart equipment manufacturers.

Get updates

Best Practices for Building Cyber-Resilient Smart Equipment

While the CRA defines minimum obligations, leading manufacturers can go further by embedding best practices:

- **Adopt secure-by-design principles.** Use secure defaults, threat modelling, and secure coding early in development.
- **Integrate cybersecurity into DevOps.** Incorporate security testing and scanning into CI/CD pipelines.
- **Plan for long-term support.** Define clear end-of-life policies, maintain infrastructure for updates, and communicate advisories to users.
- **Continuously monitor risk.** Track component reuse, monitor for vulnerabilities in libraries and dependencies, and maintain robust update readiness.

What Manufacturers Need to Do Next

To begin your journey toward CRA readiness, focus on these five practical steps:

1. **Audit your device portfolio for CRA applicability**
   Identify which connected products fall under CRA scope and assess your current security maturity. This provides a baseline for risk, compliance, and opportunity for platform support.
2. **Assess your current device management and update capabilities**
   Evaluate how updates are delivered, verified, and tracked. Modern device management platforms like Cumulocity can automate OTA updates, provide visibility into update status, and ensure audit trails.
3. **Ensure SBOM tracking and component-level visibility**
   CRA requires a full software bill of materials (SBOM) for each product. Ensure your teams can generate, manage, and use SBOMs to respond to threats in real time.
4. **See how Cumulocity can help — with our CRA Technical Guide**
   Cumulocity supports CRA-readiness through secure updates, fleet-wide software visibility, and built-in risk tracking. Our guide, A Practical Reference Architecture for Cyber Resilience Act (CRA) Compliance, includes architecture diagrams, compliance workflows, and practical implementation insights. Sign up to receive a copy.
5. **Connect with our team for a CRA-readiness discussion**
   Need to map your current posture against CRA requirements? Our product and compliance experts can help you outline next steps and identify opportunities for platform support — no sales pressure, just insights.

How Cumulocity Helps Manufacturers Meet CRA Requirements

Cumulocity provides an integrated platform that helps manufacturers meet CRA requirements across several key domains:

- Fleet-wide device visibility, including SBOM tracking
- Secure OTA update delivery, with audit trails and rollback support
- Event and anomaly monitoring (e.g. login failures, failed updates)
- CVE correlation and vulnerability tracking
- Conformity assessment support with built-in documentation tools

By using Cumulocity, manufacturers can accelerate their CRA readiness while reducing manual effort and uncertainty. Our partner ecosystem also includes consultancies who can support your security architecture and readiness planning.

Conclusion

The Cyber Resilience Act is reshaping how connected products are designed, deployed, and supported. While the regulation introduces new complexity, it also drives product security, customer trust, and market access.

Manufacturers who prepare early — and partner with platforms like Cumulocity — can not only comply, but compete more effectively in a secure and regulated future.

Take the next step

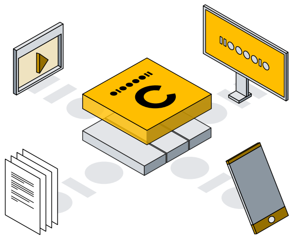
The path to CRA compliance starts with clear insight and the right tools. Don't wait until deadlines loom — take action today to secure your smart products and stay ahead of regulatory pressure.

GET EXPERT HELP

Want to understand how your current systems align with CRA requirements?

Our professional services team can help you map your readiness and identify practical next steps.

Talk to an expert



Manufacturer CRA Checklist

Manufacturer CRA Checklist

- Do your products fall within CRA scope?
- Can they receive secure updates with cryptographic verification?
- Do you maintain a software bill of materials (SBOM) for each device?
- Are you prepared to report exploited vulnerabilities within 24 hours?
- Is there a process to monitor and mitigate third-party vulnerabilities?

Resources

Official References:

- EU Cyber Resilience Act (EU 2024/2847)
- ENISA/JRC CRA Requirements Mapping Document

Glossary

- **SBOM (Software Bill of Materials):** A list of software components in a product.
- **OTA (Over-the-Air):** Remote delivery of firmware or software updates.
- **Secure Boot:** A process that ensures device integrity during startup.
- **CVE (Common Vulnerabilities & Exposures):** Publicly disclosed cybersecurity flaws.

ABOUT CUMULOCITY

We're an end-to-end AIoT platform that powers the smart connected product revolution.

Cumulocity connects & manages your assets efficiently, transforms raw device data into AI-ready data, and orchestrates innovation from cloud to edge.

Find out more

CUMULOCITY